Evaluation of Cloud Computing Offers through Security Risks
An Industrial Case Study

Jean-Michel Remiche[1], Jocelyn Aubert[2], Nicolas Mayer[2] and David Petrocelli[1]

[1]POST Telecom, 1, rue Émile Bian, Luxembourg, Luxembourg

[2]Luxembourg Institute of Science and Technology, 5, avenue des Hauts-Fourneaux, Esch-sur-Alzette, Luxembourg

Keywords: Cloud Computing, Security Risk Management, Industrial Case Study.

Abstract: Cloud provider selection is a difficult task, even more when security is a critical aspect of the processes to be moved on the cloud. To support cloud offer selection by a cloud consumer, we have introduced an innovative risk-based approach, proposing to distribute risk assessment activities between the cloud provider and the cloud consumer. This paper proposes an evaluation of this approach by assessing and comparing the portfolio of offers of POST Telecom, a cloud provider in Luxembourg. The case study will cover the evaluation of the offers with the help of standard security controls provided by three leading cloud organizations: Cloud Security Alliance, ISO/IEC and SANS Institute.

1 INTRODUCTION

Cloud computing helps companies to focus on their core business activities by transforming traditional capital expenditure (CAPEX) into operational expenses (OPEX). Its scalability and its pay-as-you-go pricing scheme allow a rapid adjustment of resources to meet unpredictable demand. So basically, cloud computing supports growth by handling costs without heavy investments, a blessing in times where cost reduction plays a vital role. On the other hand, studies and surveys demonstrate that security is a major concern for companies wanting to migrate their business processes, platforms or software to the cloud, sometimes leading to a renouncement because of lack of trust towards the provider and its offers.

In a cloud computing context, security requires solutions different to those provided by current research efforts and industrial practices. In a traditional setup, an organization's infrastructure is in a known environment that is either hosted by the organization on its own premises or is directly managed by the organization. However, when an organization's infrastructure migrates to the cloud, relevant applications and stored data are in an environment that is separated, managed and maintained externally, out of the organization's boundaries. This creates an extra set of challenges with regards to the security risk management process. To deal with these challenges, Goettelmann et al. have proposed an innovative way to perform security risk management in a cloud environment (Goettelmann et al., 2014) in order to support the selection of a cloud offer. This approach, summarized in this paper, is based on a distributed process of security risk management. It involves the cloud consumer, assessing its security needs and the impacts of potential risks on its business, and the cloud provider, assessing the vulnerabilities of its offer(s). A third actor is involved: the cloud broker that reconciles the security needs of the cloud consumer with the security level of the offer(s) through a risk-based approach, making clear if and how the considered threats harm the consumer and how well the provider deal with them. The role of cloud broker can be played by a neutral third party, as well as by the cloud provider or the cloud consumer. The objective of this paper is to report on the application of this approach in a real-world context. More specifically, we assess and compare the portfolio of offers of POST Telecom, a cloud provider in Luxembourg, composed of three offers having an increasing level of security. The case study will cover the evaluation of these three offers through the standard security controls provided by three leading cloud organizations: Cloud Security Alliance, ISO/IEC and SANS Institute.

Section 2 describes the background of our work: cloud computing and security risk management.

Remiche, J., Aubert, J., Mayer, N. and Petrocelli, D.
Evaluation of Cloud Computing Offers through Security Risks.
DOI: 10.5220/0006665703380345
In *Proceedings of the 8th International Conference on Cloud Computing and Services Science (CLOSER 2018)*, pages 338-345
ISBN: 978-989-758-295-0

Section 3 presents our innovative approach of cloud offer selection based on security risk management. Section 4 provides a comparison with related work. Section 5 reports about our case study: it presents the case studied, the conceptual framework and the evaluation results. Finally, conclusions and future work are presented in Section 6.

2 BACKGROUND

This section aims at introducing the concepts at stake and the evaluated approach. We first present the concepts and key characteristics of cloud computing. Then, we highlight the difficulty of using security risk management in an organization deploying some of its business processes in the cloud.

2.1 Cloud Computing

Cloud computing has become a mainstream technology offering mutualisation of IT infrastructures as services along several paths such as Software (SaaS), Platform (PaaS), and Infrastructure (IaaS) (Vaquero et al., 2008). It thus enables **cloud consumers** to consume resources (virtual machine, storage or application) provided by **cloud providers**, just like any other utility (e.g., electricity) rather than having to build and maintain their own in-house computing infrastructures.

This incontestable advantage, coupled with on-demand provisioning, elasticity as well as pay-per-use, allows organizations to focus on their own core business activities instead of their system infrastructures (Armbrust et al., 2009). It is therefore obvious that cloud computing is of great benefit for organizations, especially in times where cost reduction plays a vital role. Nevertheless, given security attacks and other data breaches targeting cloud computing services (Kolevski and Michael, 2015) that occurred in recent months, the use of such services clearly exposes users to a certain number of risks. Different taxonomies of such risks have been published, notably by CSA (Brook et al., 2016) and ENISA (European Network and Information Security Agency, 2009a). If for a majority of these risks, their existence seems independent of the use of cloud computing services, some new kinds of risks appear: risks that would not rise within on-premises deployment. To illustrate, this is the case for policy and organizational risks (including lock-in, loss of governance, service termination, etc.) but also for legal risks (including subpoena, changes of jurisdiction, licensing risks, etc.).

Accordingly, in order to tackle these risks, a risk management approach suited to this paradigm and taking into account its specificities should be adopted. Otherwise, businesses will remain vulnerable to potential security breaches that could result in greater loss than expected gains made by the switch to cloud technology.

2.2 Security Risk Management

Where the business processes of an organisation run locally (on-premises) and not in a cloud infrastructure, the implementation of a security risk management approach (ISO/IEC, 2011) is yet complex but globally well understood. Business processes are supported by the resources controlled by the organisation (i.e., *supporting assets*) and have security objectives related to their criticality. These assets can have various vulnerabilities which, combined with different threats, generate security risks for the organisation. From security objectives and risk perspective, security requirements are deduced for mitigating these security risks. Traditionally, these are mainly implemented, on the one hand by constraints on the business processes (business processes evolution for supporting security requirements), and on the other hand by constraints on the supporting assets (modification of the architecture, additional security controls, etc.).

In a cloud-based infrastructure, where business processes can run remotely (off-premises), the implementation of security objectives is different. In fact, if security risks can still be avoided by changing the business processes, the cloud cannot be constrained as easily (if even possible) as local assets, because it is not controlled by the organisation itself (Goettelmann et al., 2013). As a consequence, cloud specific security risks, as explained by ENISA (European Network and Information Security Agency, 2009a), cannot be managed so easily. However, if the consumer company cannot control the cloud risks, it has the power to select the cloud provider (resp. the specific offer of a cloud provider) that better fulfils its security requirements. Subsequently, this supposes that providers expose different and negotiable guarantees regarding security that are implemented through security controls, and that these guarantees can be compared based on reliable metrics, possibly provided by trusted third parties. These principles are discussed in the approach overviewed in the next section.

3 RISK-BASED CLOUD OFFER SELECTION

The approach evaluated in this paper has been defined by Goettelmann, and this section, aiming at presenting it, is taken from his PhD thesis (Goettelmann, 2015). The approach relies on the assumption that cloud security risks cannot be fully assessed by neither the cloud consumer, nor the cloud provider on their own. A security risk can be defined as the combination of a **threat** with one or more **vulnerabilities** leading to a negative **impact** harming one or more of the assets (ISO/IEC, 2011). The evaluation of these three risk components has to be split over the different cloud actors, as explained below. Initially, the **impact** can only be defined by the cloud consumer, as the owner of the business that is affected by a potential security breach. When an incident occurs (such as for example a "data breach" or a "denial of service" attack), the consequences directly affect the cloud consumer's processes. The cloud provider does not necessarily know if the consumer's data are for example confidential or if the service is only used for a testing purpose. Therefore, to properly assess the final risk value, the impact value has to be evaluated from the perspective of the cloud consumer.

On the other side, the **vulnerabilities** are given by the cloud provider, since it is his system that can have security flaws and allow an incident. The infrastructure (platform or software) of the cloud service is under the responsibility of the provider. It is difficult for a cloud consumer to identify possible vulnerabilities, since mostly he/she is not familiar with the technology behind the used services. In opposition to an on-premises infrastructure, where the information system is under full control and can be investigated for security weaknesses by the organisation itself, in a cloud environment this has to be delegated to the provider.

Finally, the cloud broker can help the cloud consumer to define the impact value and the cloud provider to secure their offers, typically by defining a set of **threats** that have to be considered. It is worth to note that the cloud broker is not necessarily an external and independent entity, it can be considered as a role that the cloud consumer or cloud provider plays. Typically, when seeing the generic cloud risk assessment as published by the CSA (Brook et al., 2016) or the ENISA (European Network and Information Security Agency, 2009a), we consider that the threat is generic and its probability independent from the two other values (the impact and the vulnerabilities).

Our model is more precisely illustrated in Figure 1. It defines the notions needed to evaluate the impact, the vulnerability and the threat before aggregating them into the final security risk value. The model can be divided into three sub-models, a consumer model, a provider model and a broker model.

The **cloud consumer** has a set of assets that are candidate for being outsourced on one or more cloud providers/offers. Assets can be of any type, software components, tools, models, or data elements. Assets should have a value, i.e., be of some importance for the company. The consumer defines a set of security criteria (typically confidentiality, integrity and availability) on which he/she specifies his security needs. This association is called a security objective.

Generally, the need of an objective corresponds to a value to classify the assets in terms of their importance. It should be understood as follows: an asset has the objective of fulfilling a security criterion which can be quantified by the need value. For example, a security objective could be: "*passwords* (asset) *should be kept secret* (high need of confidentiality) *within the company*".

The **cloud provider** considers a set of security controls that he can implement on his infrastructure or services. Controls are safeguards or.

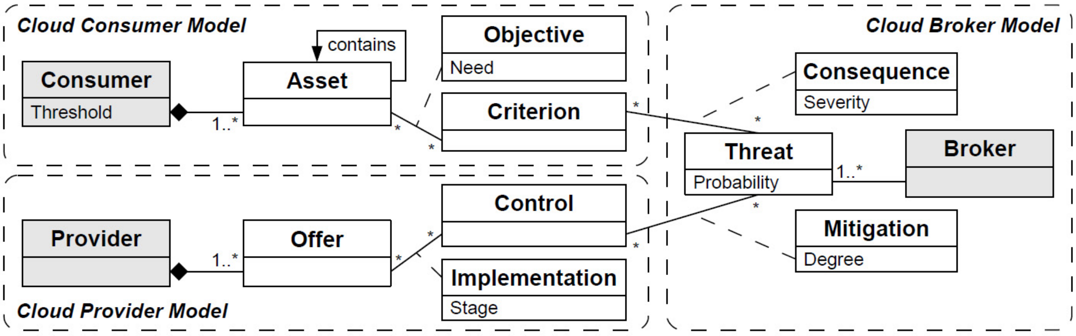

Figure 1: Risk assessment model for cloud environments (extracted from (Goettelmann, 2015).

countermeasures used to prevent the occurrence of a security incident and increase the security of the installations. As an example, a firewall or an antivirus software can be considered as security controls. The implementation of such controls can be specified in terms of a stage that corresponds to a value on a pre-defined scale. In general, this information has a binary form (True or False), but sometimes controls can be implemented gradually. The relation should be understood as follows: a cloud provider implements for each of his offers different security controls, this relation can be quantified by the stage value. As an example, "sensitive information encrypted (control) with an AES-128 algorithm (medium stage of encryption) within the company", is a form of a security control's implementation.

In accordance with the cloud consumer, the **cloud broker** defines a set of cloud security threats to consider that could adversely harm the cloud consumer's assets. On the one side, these threats have consequences that can be defined through the security criteria (e.g., some threats will affect the confidentiality of a resource, and others more the availability). This relation can be specified in terms of severity of the consequence. It should be understood as follows: each threat has a consequence on the security criteria that can be quantified by the severity value. As an example, "*a denial of service attack* (threat) *temporarily suspends* (high severity in terms of availability) *the provided service*", is a quantified consequence of a threat. On the other side, these threats can be mitigated by security controls that counter the security flaws permitting those threats. This relation can be specified in terms of a degree. It should be understood as follows: each security control is intended to mitigate one or more threats, the mitigation level being quantified by the degree value. As an example, "*systematic background checks* (control) *on new employees significantly reduce* (high degree of mitigation) *the risks generated by a malicious insider* (threat) *within a company*", is a form of a quantified threat mitigation.

4 RELATED WORK

The literature is rich with research efforts that consider security and risk issues within the context of cloud computing. A broad and detailed analysis of the related work has been done (Goettelmann, 2015), but cannot be presented here for sake of brevity. Among what we consider as the most related works, Gillam et al. incorporate quality of service into cloud Service Level Agreement (SLA) (Gillam et al., 2012); in particular this work measures QoS to predict availability, quantify risk, and consider liability in case of failure. Islam et al. introduce a risk management framework to support users with cloud migration decisions (Islam et al., 2017). This framework enables users to identify risks, based on the relative importance of the migration goals and analyzed the risks with a semi-quantitative approach. Wenzel et al. consider security and compliance analysis of outsourcing services in the cloud context (Wenzel et al., 2012). The work initially considers risk analysis of business processes that are planned to be outsourced and if the process is outsourced then compliance issues are checked. The final part of the approach involves security analysis of the physical distribution of the process and communication among the entities. Khajeh-Hosseini et al. introduce a cost, benefits and risk tool as decision support for public IaaS cloud migration (Khajeh-Hosseini et al., 2011). The cost modelling tool enables user to model IT infrastructure using UML. Risks are considered from organisational, legal, security, technical and financial perspectives. Finally, Stamou et al. propose an approach to select cloud offers based on a risk assessment method (Stamou et al., 2012). In these preceding works, the focus of risk assessment is put on the cloud provider and it does not support the elicitation of security requirements from the cloud consumer, as well as its reconciliation with the security offered by the cloud providers to select the most suited offer. We consider with our approach that a cloud consumer should be able to assess the level of security of several cloud offers and select the most adequate one with respect to its security requirements having the capability to implement its business processes.

To another extend COAT (Alnemr et al., 2014) matches user's non-functional requirements to cloud offers and performs a comparison of these cloud offerings. Our approach differs in that we only focus on a part of non-functional requirements (i.e., security) but on the other hand we facilitate the expression of these requirements using a risk-based approach.

Recent initiatives mainly from the industry and government organisations have sought to produce a number of guidelines and methods to help in the selection of cloud providers as well as addressing some specific security concerns of the cloud (European Network and Information Security Agency, 2009b; ISO/IEC, 2015; National Institute of Standards and Technology, 2011; Winkler, 2011).

Yet such guidelines appear often too cumbersome with no clear indications as to when a cloud service provider may be considered as not being trustworthy. This makes the valuable information detailed within these documents hard to exploit without an additional methodological approach.

5 EVALUATION OF THE APPROACH

The objective of the paper is to evaluate with the help of an industrial partner the cloud provider side of the approach, i.e., the Cloud Provider Model as well as its directly linked concepts in the Cloud Broker Model (*Threat* and *Mitigation* in Figure 1). Our aim is to report on its application with different cloud offers and different cloud security reference model and then elaborate on lessons learned. In this section, we first present our case, then the conceptual framework established, and finally the evaluation results on actual offers.

5.1 Overview of the Case

POST Luxembourg is the largest provider of postal and telecommunications services in Luxembourg. Its telecommunications services range from landlines and mobiles to internet and television, as well as many specially designed services for businesses. As part of its portfolio of services, POST offers a full range of cloud services such as IP telephony, email, sharing spaces, virtual desktops, etc. These services can be accessed via a public cloud infrastructure named *CloudBizz*. Different versions have been designed and are currently proposed to clients, each having a specific level of security.

POST Telecom is currently facing two specific challenges that are related to our research work. First, POST Telecom wants to adopt a more client-centric approach by making clear the risk coverage of each version of *CloudBizz*. Such an approach is deemed as necessary to justify the inclusion of advanced (and sometimes costly) security controls. Second, it wants to ensure that clients have the opportunity to clearly compare offers coming from competitors, in a neutral, sound and standard manner.

5.2 Conceptual Framework

The risk assessment model depicted in Figure 1 is implemented in a Microsoft Excel workbook, with different macros written in Visual Basic for Applications (VBA). This tool is named the CSRA (Cloud Security Risk Assessment) tool. The tool is evaluated with three cloud security reference models:

The **Cloud Controls Matrix (CCM)** (Cloud Security Alliance, 2014) a set of controls proposed by the Cloud Security Alliance (CSA), an organization dedicated to defining and raising awareness of best practices to help ensure a secure cloud computing environment. The CCM proposes a list of security controls to reduce security threats bound to cloud computing.

The **ISO/IEC 27017** international standard gives guidelines for information security controls applicable to the provision and use of cloud services. It includes a list of security controls cloud providers should implement in order to reach a standard security level.

The Center for Internet Security (CIS) has published the **CIS Critical Security Controls (CIS Controls)** that are a concise, prioritized set of cyber practices created to stop today's most pervasive and dangerous cyber attacks.

Three different versions of the *CloudBizz* solution are the analysed offers: *Basic:* the original version of the solution, *Advanced:* an improvement of the original version including additional security controls, and *Finance:* a sector-specific and more secure version, complying with the security requirements of the Luxembourg's financial regulator.

The set of considered threats is the one identified by the CSA as the top threats to cloud computing (Cloud Security Alliance, 2013) and called "*The Notorious Nine*". One can argue that a more exhaustive list of threats could have been defined and used. However, due to available standards focused specifically on these threats, we decided to limit this first evaluation to this set of threats, but we consider that to extend the considered threats is a must have in an industrial context.

A two-step process is followed in order to determine the risk coverage of an offer with regards to a cloud security reference model. The evaluators were the Chief Information Security Officer and the Head of ICT & Cloud Solutions at POST Telecom S.A. having performed together each evaluation with the CSRA tool.

5.2.1 Evaluation of Implementation Stages

In this step, the evaluators play the role of cloud provider and evaluate the implementation of each security control. This step is performed nine times –

one for each combination of a cloud offer with a cloud security reference model. The scale used to determine the implementation stage of each control is: **0** if not implemented, nothing is in place for this control (e.g., a two-factor authentication for all remote login access is a standard control (System Administration Networking and Security Institute, 2015) that has not been implemented); **0.5** if half-implemented, control in place but room for improvement to reach a state-of-the-art level (e.g., information security awareness, education and training (ISO/IEC, 2015) is a control that has not been established for all resources yet and that is still in progress); and **1** for fully implemented, a state-of-the-art control is in place (e.g., a full access management process (ISO/IEC, 2015) is a control that has been fully implemented through a self-service portal).

5.2.2 Definition of Mitigation Degrees

In this step, the evaluators play the role of cloud broker and specify the mitigation degree of each security control with regards to the cloud specific threats of "*The Notorious Nine*". This step is performed three times – one for each cloud security reference model.

For each threat, the mapping between the set of standard controls defined by the CSA and the analysed threats is extracted from the Cloud Controls Matrix (CCM). Then, thanks to mappings between the CSA controls and ISO/IEC 27017 (Cloud Security Alliance, 2014), and the CSA controls and CIS controls (System Administration Networking and Security Institute, 2015), we are able to link security controls of the two other cloud security reference models with the threats.

The current standards consider that each control associated to a threat has the same mitigation degree. Although it is an approximation, we decided to follow this assumption and stick at the level of information provided in current standards.

To report on the results, we benchmark the use of the three cloud security reference models tested in our approach. To do so, we measure for each of these reference models the evolution of the threat coverage and compare it with the evolution of the implemented controls. The threat coverage is measured by combining the implementation stage and the mitigation degree of the controls actually implemented while the evolution of the implemented controls is measured by computing for each pair of offers, the variation of the ratio of controls actually implemented.

5.3 Results

The result of the evaluation consists in 9 filled instances of the CSRA tool: one for each combination {*CloudBizz Solution version, Cloud security reference model*}. Each of these instances of the CSRA tool depicts the coverage level of the nine threats by the controls (of a specific cloud security reference model) implemented in the studied cloud offer.

The three different offers were studied in terms of threat coverage. The histogram part of Figure 2 shows the average threat coverage expressed in percentage of the three offers for the three reference models. Regardless of the reference model used; the *Finance* offer has a better threat coverage than the *Advanced* offer, which has a better coverage than the *Basic* offer. For confidentiality reason and sake of brevity, only the average threat coverage values are illustrated here, but the same is true for the individual values of each threat for the three offers.

By putting into perspective the evolution of the threat coverage on the one hand, and the evolution of the implementation of the controls of the various reference models on the other hand (Figure 3), a relevant finding can be noted. When switching from the *Basic* offer to the *Advanced* one, the evolution of threat coverage is higher than the evolution of the implementation (average ratio implementation/threat

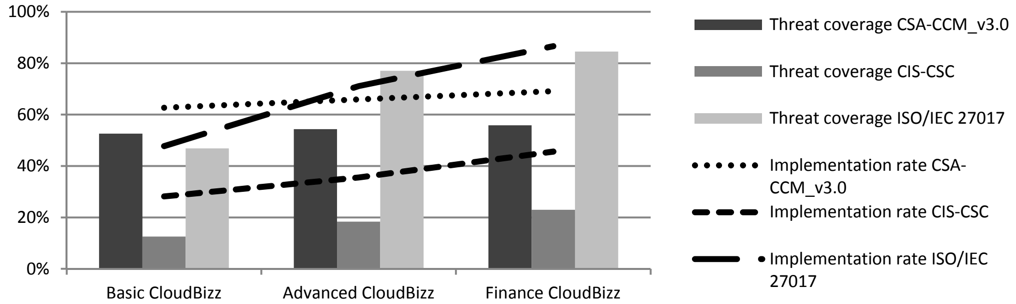

Figure 2: Threat coverage of offers compared to offer implementation.

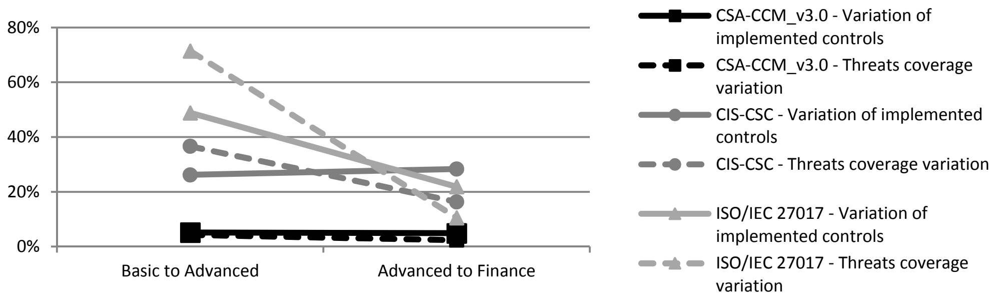

Figure 3: Variation of offer implementation and threat coverage by offers.

coverage being around 1.23), whereas this reverses when switching from the *Advanced* offer to the *Finance* one (average ratio implementation/threat coverage being around 0.52).

Besides, by focusing neither on the rate of evolution of the implementation but on the completeness of implementation of the offers with regard to the different reference models (that is to say for an offer, the ratio of actually implemented controls of a given reference model), a heterogeneity of the levels of implementation between different reference models can be observed for a same offer as illustrated in line part of Figure 2.

Table 1: Offers' efficiency by reference model.

	CSA-CCM_v 3.0	CIS-CSC	ISO/IEC 27017
Basic CloudBizz	0.84	0.45	0.98
Advanced CloudBizz	0.82	0.52	1.00
Finance CloudBizz	0.81	0.50	0.98
Average	**0.82**	**0.49**	**0.99**
Median	**0.82**	**0.50**	**0.98**

By combining this implementation rate with the threat coverage for each pair {*reference model, offer*}, the efficiency of an offer towards threats mitigation can be obtained. Considering as an initial hypothesis that an offer fully implementing a reference model (implementation rate: 100%) offers a complete mitigation for the nine threats used as reference (threat coverage: 100%), the efficiency (ratio threat coverage/implementation rate) tends to 1. Table 1 presents the efficiency of the offers for each reference model. It can be seen that CSA-CCM and ISO/IEC 27017 have a median efficiency close to 1 (respectively 0.82 and 0.98) for the three offers while CIS-CSC has a lower efficiency (around 0.50).

Based on these observations, the following conclusions can be drawn. In the first place, based on the fact that the three distinct offers have an increasing level of security and that the threat coverage values obtained are gradual (Figure 2): a more secure offer gives a better threat coverage. Thus the three reference models enable to make clear the risk coverage of a given offer and allow a coherent comparison of different offers.

The efficiency of the offers make possible to highlight the adequacy of a reference model to benchmark an offer. In this sense, ISO/IEC 27017 and CSA-CCM seem to be most suitable than CIS-CSC. However, this should be balanced by the fact that CIS-CSC, by definition, does not allow a full coverage (the threats *Data Loss* and *Abuse of Cloud Services* are not covered at all). This is explained by its more technical orientation. Finally, the fact that from a certain level of threat coverage, the effort to be provided (i.e., implementation of new controls) is greater than the gain of threat coverage highlights the possibility of determining an optimal level of improvement by reference model and by offer. Such information would undoubtedly be relevant both to the cloud provider and the consumer.

5.4 Threats to Validity

We have identified different threats to validity. Firstly the evaluators of the approach were employees of the cloud provider, and in charge of securing cloud offers. In order to make this industrial case study possible, it was necessary to have them as evaluators (they know how the cloud offers are designed), but the same evaluation led by external people could have produced different results.

Secondly, we considered only nine threats. To be representative of real-world considerations, many more threats should have been considered. However, “The Notorious Nine” have the advantage to be a documented standard. By adding other threats, we would have to define our own mapping between these threats and the standard controls mitigating these threats that would have been another threat to validity.

Lastly, the assumption (done by Cloud Security Alliance) that each control associated to a threat has the same mitigation degree is a threat to validity in the sense that control effectiveness to mitigate a threat can be different from one control to another. However, as introduced above, although it is an approximation, we decided to follow this assumption to stick at the level of information provided in current standards and avoid introducing our own proposal, arguable by design.

6 CONCLUSIONS AND FUTURE WORK

In this paper, we have evaluated our risk-based approach for cloud offer selection using the portfolio of offers of a Luxembourg cloud provider. The results demonstrate the applicability of such an approach and its adequacy to make clear the risk coverage of offers.

Regarding future work, we want to evaluate also the cloud consumer part of our approach. To do so, it is necessary to develop a Cloud Consumer Model (CCM) that will be supported by a Security Requirements Engineering (SRE) approach. A second aspect will be to develop a risk-based decisional model to support the cloud consumer during its offer selection. In this sense, Multiple Criteria Decision Analysis (MCDA) (Belton and Stewart, 2002) will be investigated.

REFERENCES

Alnemr, R., Pearson, S., Leenes, R., Mhungu, R., 2014. Coat: Cloud Offerings Advisory Tool, in: *2014 IEEE 6th International Conference on Cloud Computing Technology and Science (CloudCom), Singapore, Singapore, 15 - 18 December, 2014*.

Armbrust, M., Fox, A., Griffith, R., Joseph, A.D., Katz, R.H., Konwinski, A., Lee, G., Patterson, D.A., Rabkin, A., Zaharia, M., 2009. *Above the Clouds: A Berkeley View of Cloud Computing*.

Belton, V., Stewart, T., 2002. Multiple Criteria Decision Analysis: An Integrated Approach. *Springer Science & Business Media*.

Brook, J.-M., Field, S., Shackleford, D., Hargrave, V., Jameson, L., Roza, M., 2016. The Treacherous 12: Cloud Computing Top Threats in 2016. *Cloud Security Alliance.*

Cloud Security Alliance, 2014. Cloud Control Matrix (CCM) v.3.0.1. *Cloud Security Alliance*.

Cloud Security Alliance, 2013. The Notorious Nine - Cloud Computing Top Threats in 2013. *Cloud Security Alliance.*

European Network and Information Security Agency, 2009a. *Cloud Computing Risk Assessment*.

European Network and Information Security Agency, 2009b. Benefits, risks and recommendations for information security. European Network and Information Security Agency.

Gillam, L., Li, B., O'Loughlin, J., 2012. Adding Cloud Performance to Service Level Agreements. Presented at the *2nd International Conference on Cloud Computing and Services Science, Porto, Portugal, 18 - 21 April, 2012*.

Goettelmann, E., 2015. Risk-aware Business Process Modelling and Trusted Deployment in the Cloud. *Université de Lorraine.*

Goettelmann, E., Mayer, N., Godart, C., 2014. Integrating Security Risk Management into Business Process Management for the Cloud, in: *IEEE 16th Conference on Business Informatics, CBI 2014, Geneva, Switzerland, July 14-17, 2014 - Volume 1.*

Goettelmann, E., Mayer, N., Godart, C., 2013. A general approach for a trusted deployment of a business process in clouds, in: *Fifth International Conference on Management of Emergent Digital EcoSystems, Luxembourg, Luxembourg, October 29-31, 2013.*

Islam, S., Fenz, S., Weippl, E., Mouratidis, H., 2017. A Risk Management Framework for Cloud Migration Decision Support. *Journal of Risk and Financial Management 10, 10.*

ISO/IEC, 2015. ISO/IEC 27017, Information tech., Security techniques, Code of practice for information security controls for cloud computing services based on ISO/IEC 27002.

ISO/IEC, 2011. ISO/IEC 27005, Information tech., Security techniques, Information security risk management.

Khajeh-Hosseini, A., Sommerville, I., Bogaerts, J., Teregowda, P., 2011. Decision Support Tools for Cloud Migration in the Enterprise, in: *2011 IEEE International Conference on Cloud Computing (CLOUD).*

Kolevski, D., Michael, K., 2015. Cloud computing data breaches a socio-technical review of literature, in: *2015 International Conference on Green Computing and Internet of Things (ICGCIoT).*

National Institute of Standards and Technology, 2011. *Special Publication 800-144: Guidelines on Security and Privacy in Public Cloud Computing. National Institute of Standards and Technology.*

Stamou, K., Morin, J.-H., Gâteau, B., Aubert, J., 2012. Service Level Agreements as a Service - Towards Security Risks Aware SLA Management, in: *2nd International Conference on Cloud Computing and Services Science, Porto, Portugal, 18 - 21 April, 2012.*

System Administration Networking and Security Institute, 2015. The CIS Critical Security Controls for Effective Cyber Defense (No. Version 6.0). *System Administration Networking and Security Institute.*

Vaquero, L.M., Rodero-Merino, L., Caceres, J., Lindner, M., 2008. A Break in the Clouds: Towards a Cloud Definition. *SIGCOMM Comput. Commun. Rev. 39.*

Wenzel, S., Wessel, C., Humberg, T., Jürjens, J., 2012. Securing Processes for Outsourcing into the Cloud, in: *2nd International Conference on Cloud Computing and Services Science, Porto, Portugal, 18 - 21 April, 2012.*

Winkler, V. (JR), 2011. Securing the Cloud: Cloud computer Security techniques and tactics. *Elsevier.*